

METHOD AND APPARATUS FOR HYBRID GROUP KEY MANAGEMENT

Abstract

A system for group key management including a keying material infrastructure including a root portion configured to store a root public key, a key encryption key portion operatively connected to the root portion configured to store a traffic encryption key encrypted using a symmetric key encryption key, and a public key encryption key, and a first client operatively connected to the key encryption key portion configured to store the symmetric key encryption key encrypted using a first client symmetric key, and a first group member configured to access the traffic encryption key using the first client symmetric key.

60675_3.DOC